China Blockchain Conference

借天领地：广播网络能否破解区块链的“三元悖论”？

刘肖凡、李幼平

东南大学　计算机科学与工程学院

区块链技术的本质

- 能够进行存储和计算任务的分布式系统
- 所有任务都由许多人同时完成、交叉验证

形成“值得信赖的世界计算机”

这台“世界计算机”的最大缺陷

效率低下

三元悖论的定义和解读

Currently, in all blockchain protocols each node stores all states and processes all transactions. This provides a large amount of security, but greatly limits scalability: a blockchain cannot process more transactions than a single node can. … However, this poses a question: are there ways to create a new mechanism, where only a small subset of nodes verifies each transaction? As long as there are sufficiently many nodes verifying each transaction … the system can process many transactions in parallel?

The trilemma claims that blockchain systems can only at most have two of the following three properties:

***Decentralization** (defined as the system being able to run in a scenario where each participant only has access to O(c) resources, i.e. a regular laptop or small VPS)*

***Scalability** (defined as being able to process O(n) > O(c) transactions)*

***Security** (defined as being secure against attackers with up to O(n) resources)*

虽然不严谨，但是提供了一个思路。

如果想要提高O(n)，我们应该怎么办？

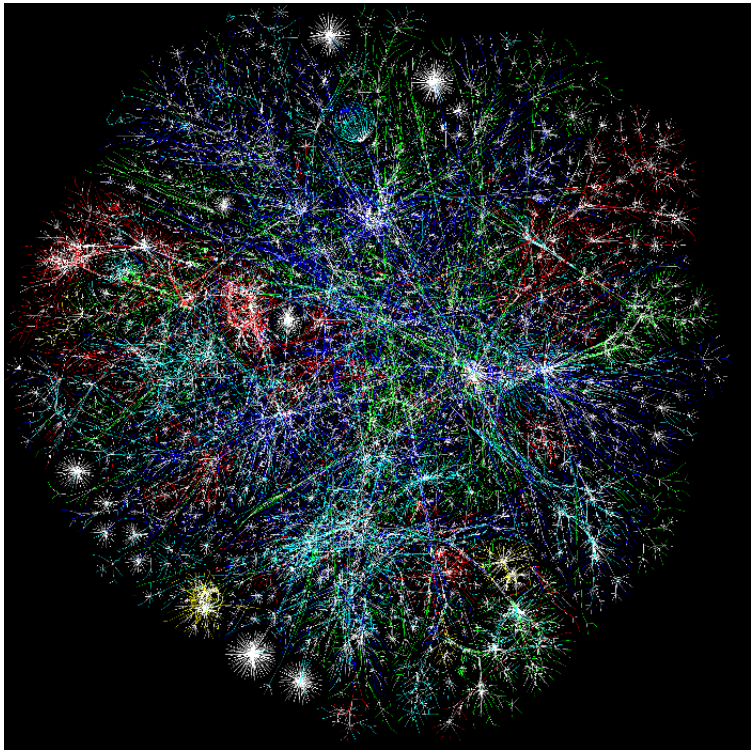
第一个思路：拆分全网任务

分为 K = O(n / c) 份分别完成，然后再拼接起来

第二个思路：增加节点能力

提升每个节点的计算、存储、网络等资源

提升网络资源的难处



英特网是一个平均距离为12跳的长尾网络

提升节点的接入带宽并不能提高网络的效率

基于卫星的全球广播网络

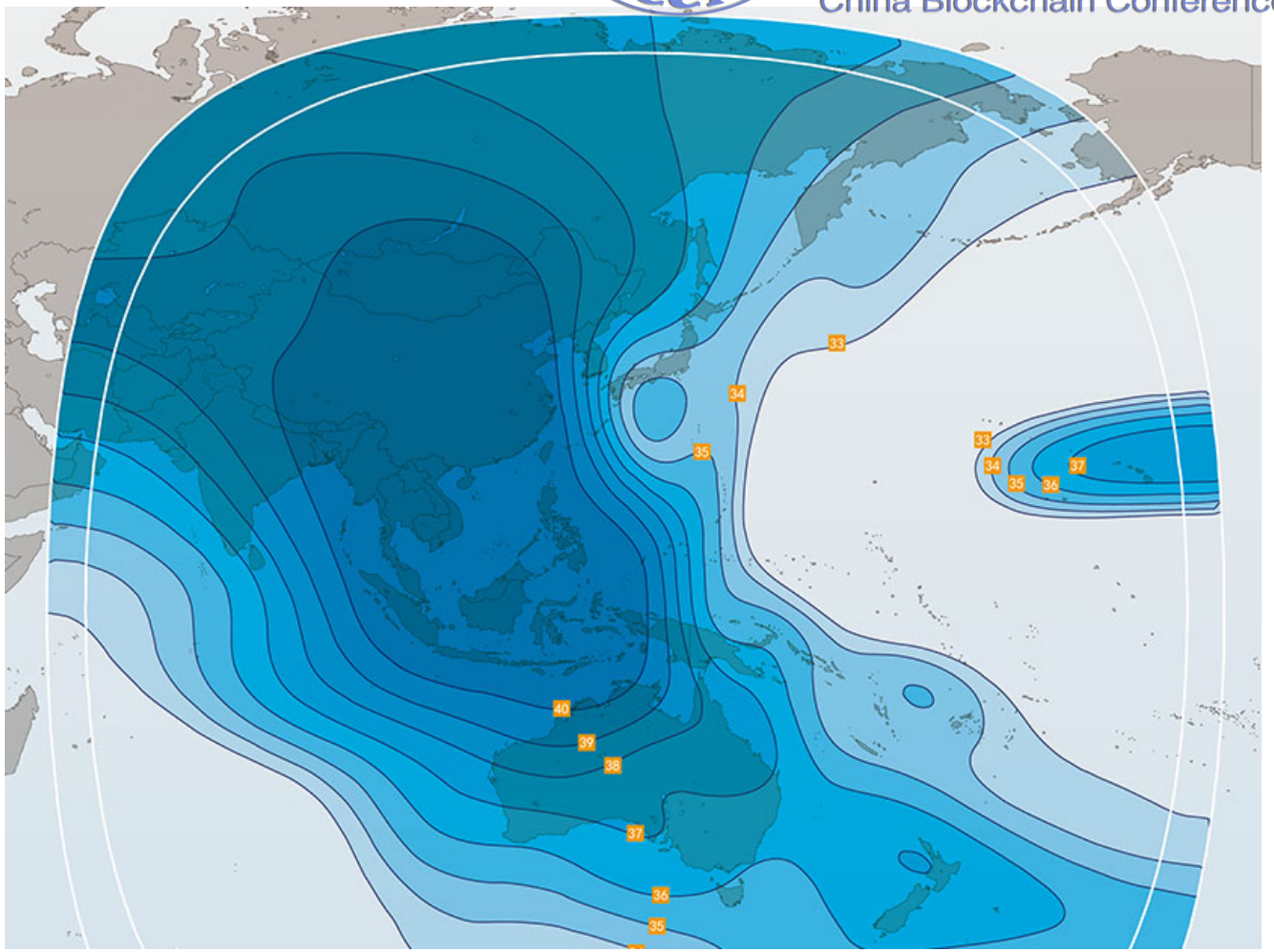
双结构互联网的构想（和实施）

当今的互联网

- Primary
- 地址驱动网络
- 随机图网络
- 互联互通 全面周到
- 侧重于地面开发
- 用户搜索信息

新添 第二网络

- Secondary
- 内容驱动网络
- 规则图网络（广播）
- 专门用于 共享共治
- 借天领地 天地一体
- 信息自寻用户



例：亚太6C卫星，C波段覆盖范围

2018年1月23日

中国首颗高通量通信卫星实践十三号在轨交付

- Ku波段，带宽20Gbps以上
- 同时传送几十部4K超高清电视节目

实践十八号，虽然发射失败

- Ka波段，带宽70Gbps以上

虽然和光纤的传输速率不能相提并论

但重要的是

1. 信息可以同时到达所有地方

2. 可以不限规模（scale-free）地复制

相当于网络资源O(c)无限大

广播对解决CAP问题的帮助

CAP定理指的是在一个分布式系统中：

- Consistency（一致性）
- Availability（可用性）
- Partition tolerance（分区容错性）

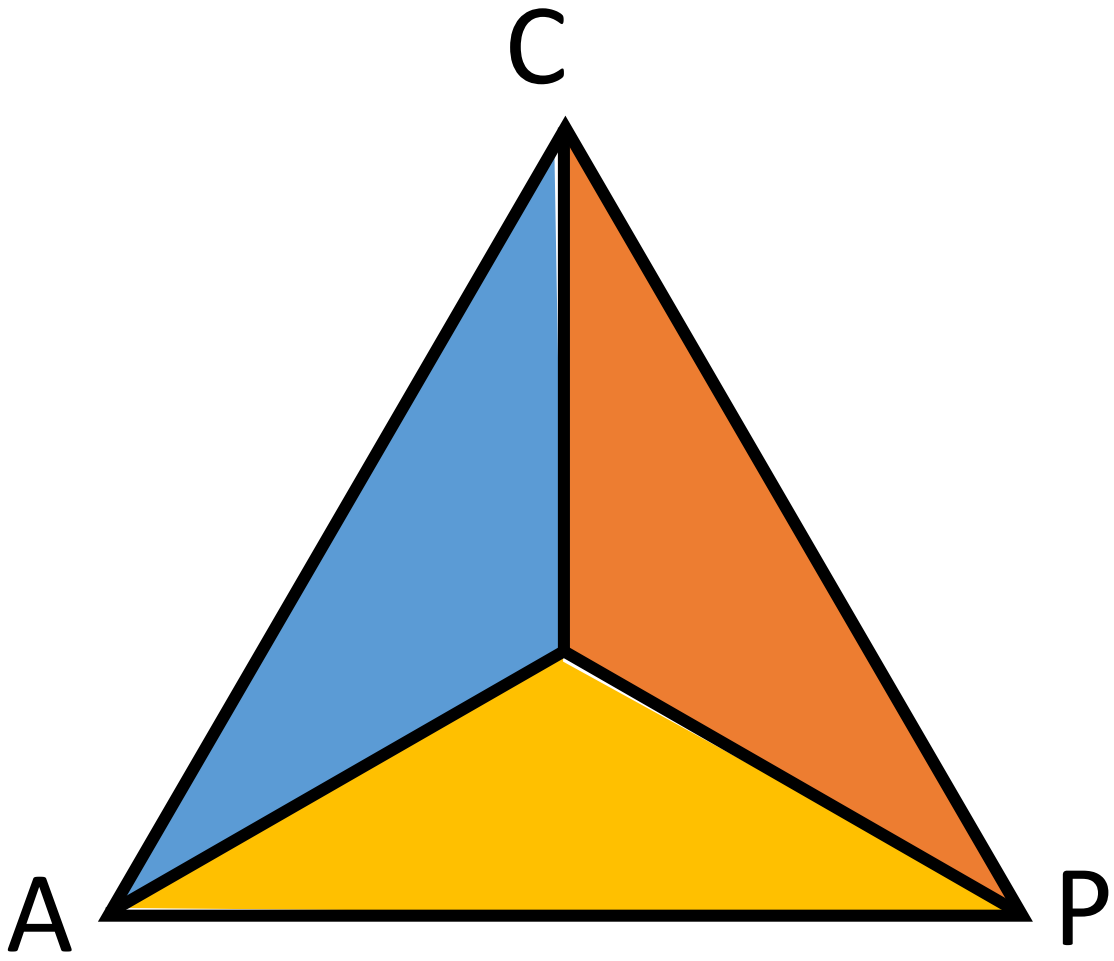
三者不可得兼

- P的具体定义是“*the network will be allowed to lose arbitrarily many messages …*"
- C和A的矛盾在于“*it is impossible … to implement an atomic … that guarantees a response …*"

区块链网络是一个典型的分布式系统
提供开放的读写和计算服务

比特币基于PoW的区块链技术实现了
- 在保证节点可用性的前提下（A）
- 达到数据“最终一致性”（C）

无论是PoS，还是PBFT等算法
都是在CAP的C和A之间进行了取舍


C
A
P

互联网和广播网中的P问题

多跳路由的互联网

- 数据乱序
- 不可预测延迟
- 丢包

解决方法复杂

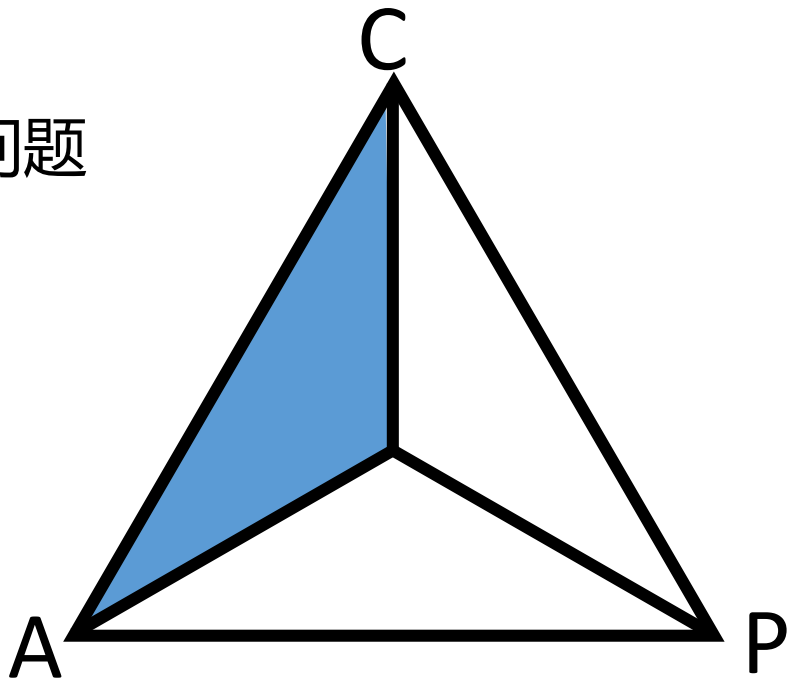
单跳传输的广播网

- 线路自然排序
- 可预测延迟
- 丢包

解决方法相对简单

广播网络

- 不仅大幅提升了节点的网络资源
- 而且减缓了由于网络不稳定带来的问题
- 使得同时保障C和A成为可能



数理互证提供广义可信数据

区块链技术的不完备性

缺乏输入正确性的证明

所谓“数理互证”指的是

实体世界与网络空间的唯一映射

但是“真实性-唯一性-可信性”的数据链条

还暂未广泛实现

国家标准UCL

China Blockchain Conference

- 国家标准《统一内容标签格式规范》（UCL，GB/T35304-2017）由东南大学和北大清华起草，中央党校大有实室负责天地测试
- 2018年4月开始生效
- 查验文件涉及人、事、物、时、位五要素是否可信无异
- 确保“数据无篡改，要素无造假”
- 做到“网络自证可信”
- 天地一体，借天领地，体现公正法制的核心价值观

终极目标：人类互信共同体

谢谢！